Information Services Board Briefing Paper on Statewide Information Technology Security

Prepared by Mary Lou Griffith, DIS/MOSTD, (360) 902-2978.

Description

Digital government requires a secure and trustworthy environment for conducting sensitive transactions through open networks. To that end, the Information Services Board (ISB) initiated a comprehensive review and update of the statewide Information Technology (IT) Security Policy to address the security issues of conducting electronic commerce across the state enterprise. The IT Internet Security Program Charter was developed and approved at the June 12, 2001, ISB meeting. A recommendation that an Independent Security Analyst be assigned to report the status of the state's IT Security Program on a recurring basis was also approved by the Board at that time. Mr. Jeff Scheel was named as the ISB Independent Security Analyst and will report the current status of the IT Security program to the Board.

Background

Washington State government has been recognized as a leader in applying digital technologies and the Internet in service to the citizen. This has been achieved by leveraging the open architecture of the Internet to provide access to a wide range of public information and services.

Using the Internet to its greatest advantage requires a higher degree of security than was the case in an earlier era of closed systems and proprietary networks. Washington State government must take sufficient steps to ensure that citizens and businesses interacting with public agencies are protected by the appropriate information technology security. Beyond a range of anonymous exchanges available through the Internet, citizens and businesses need secure access to look up their medical or other benefit claims, exchange sensitive health records, and make or receive electronic payments with government. All these transactions require secure access control and data protection for the electronic exchange of information over the Internet. This is being done through the state's secure gateway, Transact Washington, which implements trustworthy access control through Public-Key Infrastructure (PKI).

Washington State government has set a clear direction and minimum standards for the way in which sensitive information and transactions must be protected by state agencies. The policies, standards, and guidelines set the preconditions for achieving a consistent and reliable set of protections for sensitive information within a shared, trusted environment.

Status

The annual compliance letter regarding their respective information technology security programs was due from each agency head on August 31, 2002. Following the receipt of the letters, agencies were sent acknowledgment letters on behalf of the ISB and have been reminded that a compliance audit of their security programs performed by an independent auditor must be done prior to October 6, 2003. DIS hosted a security audit seminar presented by the State Auditor's Office on January 22, 2003. DIS is also assisting small agencies with preparation of their security programs to be prepared for the audits.

Washington State has made a concerted effort to improve the security of its computer systems. One example of collaboration is the Washington Computer Incident Response Center (WACIRC). WACIRC was formed in March 2002. Since that time over 50 state agencies have assigned a representatives to participate and improve Washington State government's ability to handle computer incidents.

The WACIRC members have accomplished the following:

- Created a charter defining their goals and objectives
- Established an operational foundation
- Developed a centralized incident reporting mechanism
- Developed a solid communication plan (including an in-band and out-of-band communication network for incident information and escalation)
- Developed statewide standards for wireless LANs
- Established connectivity and access control to the State Government Network
- Developed a WACIRC Incident Response Plan
- Created the framework for a public and private WACIRC website

WACIRC will conduct a test of its plan in March 2003. A project to address the security issues associated with employees' remote access to government computer networks will be initiated in the coming months.

DIS and Department of Personnel have teamed together to work with a subcommittee of WACIRC to develop a comprehensive security training curriculum and a centralization of associated security training resources. An analysis of the compliance letters identified a gap in agencies' security awareness training. DIS has contracted for an online security awareness training course and is offering it beginning in February at no cost to agencies that have access to Inside Washington.

Issues

- None noted

Recommendation

This report is informational only.